Improving Link Resilience in Software Defined Internet of Things Networking

Rehab Alawadh, Poonam Yadav, Hamed Ahmadi

Department of Computer Science

Abstract

Deploying new optimized routing policies on routers in the event of link failure is difficult due to strong coupling between the data and control planes and the absence of topology information about the network. Because of the distributed architecture of traditional Internet protocol networks, policies and routing rules are spread in a decentralized way, resulting in looping and congestion problems. To overcome this problem, we choose Software-Defined Networking (SDN) technology to create a hybrid fast failure recovery (HFFR) framework for IoT networks based on caching the flow rules which correspond to the optimal paths in the hash table deployed in the SDN controller memory in order to reduce the computation time of the forwarding path and the load at the SDN controller.

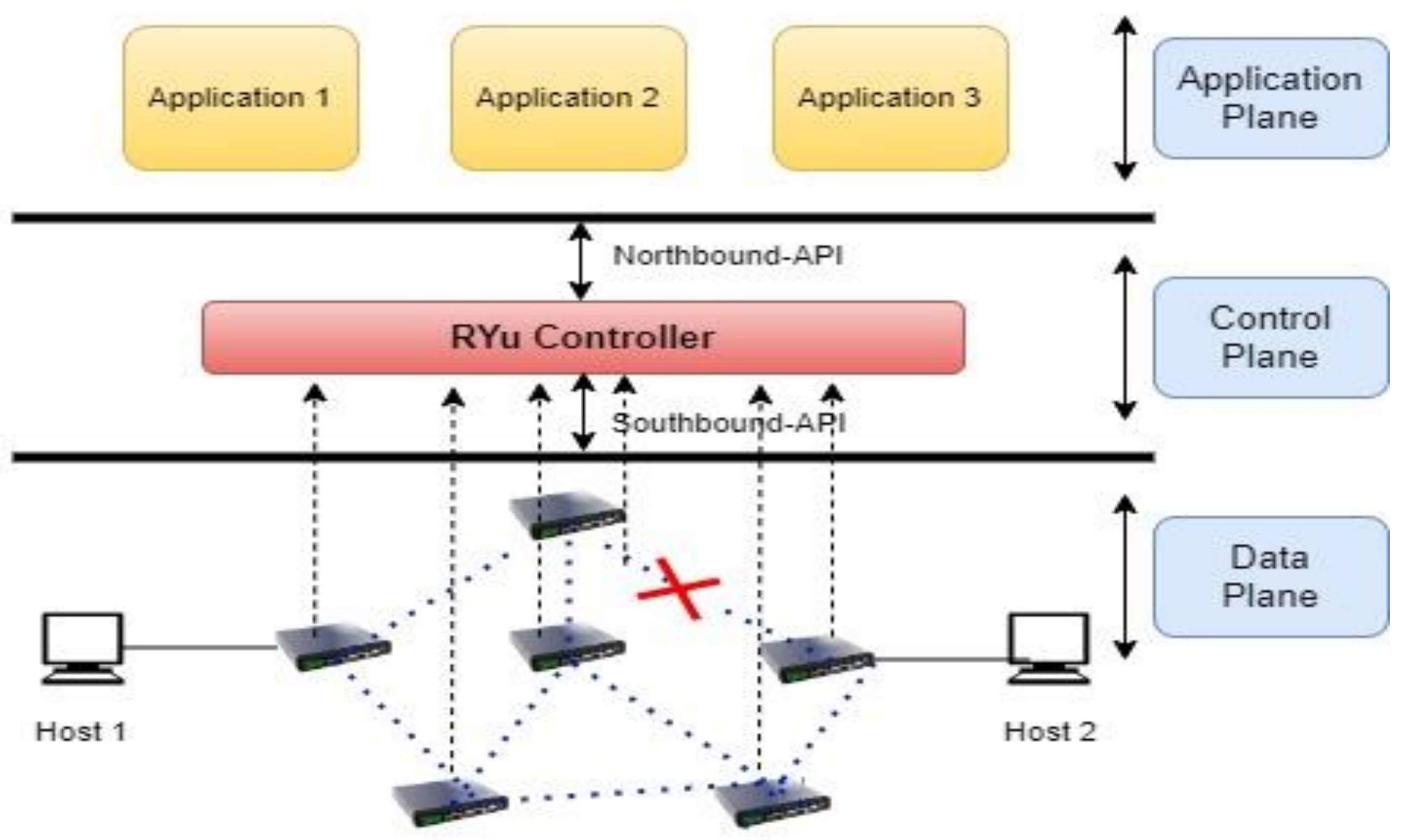
Research main concepts

Software defined networking (SDN)

SDN, or Software-Defined Networking, is a network architecture that separates the control plane from the data plane, allowing for centralized management, programmability, and dynamic configuration of network resources. It enhances network flexibility, scalability, and efficiency [1].

Link resilience in SDN

Link resilience in SDN refers to the ability of the network to maintain continuous and reliable communication by dynamically adapting to link failures, rerouting traffic, and optimizing paths through software-defined control, ensuring robust and fault-tolerant connectivity.

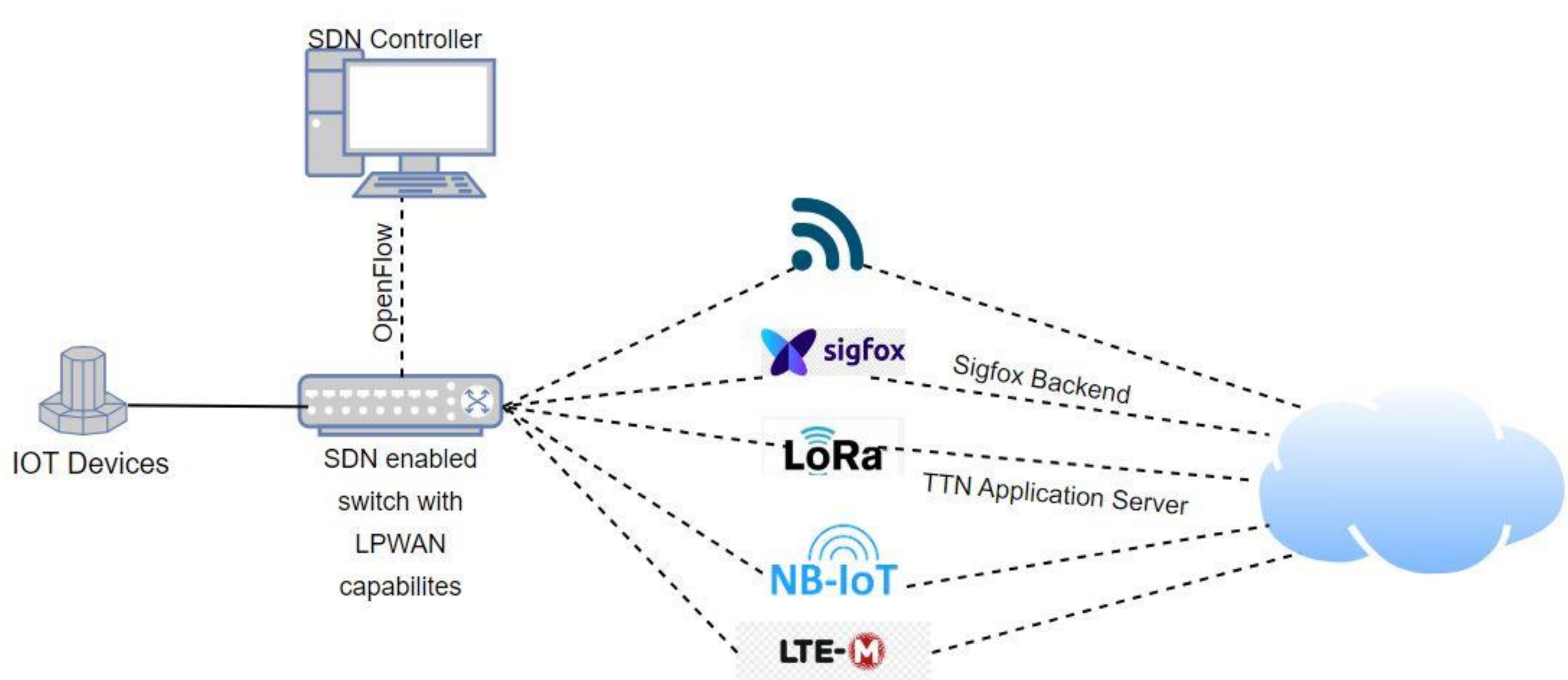


Why using hash table?

Hash tables are utilized in SDN for fast, constant-time data retrieval, optimizing network performance and facilitating efficient memory usage. They reduce both lookup and computation time for new path, supporting quick decision-making, particularly in scenarios like network recovery after failures.

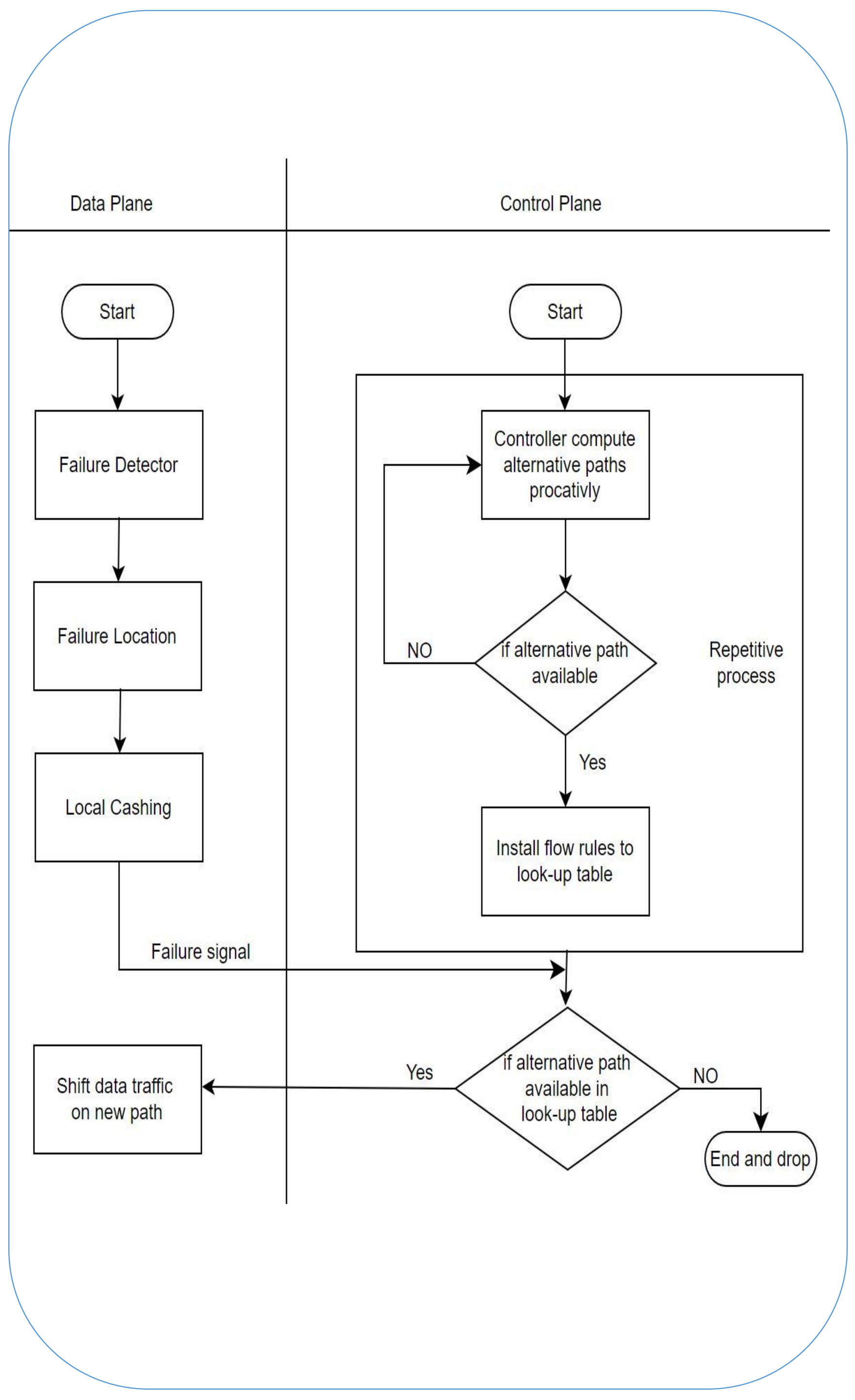
Research Problem and Solution

For IoT networks, Wi-Fi connections may experience temporary disconnections, leading to potential data loss, delays in data communication, and disruption of service availability. Therefore, network resilience in IoT devices can be improved by providing multi-network communication that allows network connectivity in case of link failure of one network medium. Low Power Wide Area Network (LPWAN) technologies have been specifically designed to meet the requirements of Internet of Things (IoT) applications.



How does HFFR work?

1. The network topology is initially stored within the SDN controller.
2. Using the network topology, the controller proactively computes an alternative path and stores it in a hash table. This minimizes the calculation time for the optimal path and reduces round-trips to the SDN controller.
3. In the event of a link failure or Wi-Fi disconnection, the data plane notifies the controller by sending a failure signal.
4. Following that, the controller transmits precomputed alternative flow entries from the hash table to the controlled devices responsible for routing flows. This eliminates the need for additional real-time calculations and resources to store alternative paths in the switches.
5. To improve the recovery process's efficiency, the controller consistently monitors alternative paths, reducing the time needed for recalculations.



System Model

Our strategy aims to find the alternative path and flow rerouting polices in case of link failed and topology been changed. This goal been achieved by sequentially monitor the network status then updating the hash table. The proposed system model consists of the next logical modules.

Main Ryu module

Is designed to provide efficient and optimized forwarding of network traffic in a Software-Defined Networking (SDN) environment. It aims to achieve this by implementing low-latency shortest path forwarding and utilizing network awareness and monitoring functionalities.

Network Awareness Module

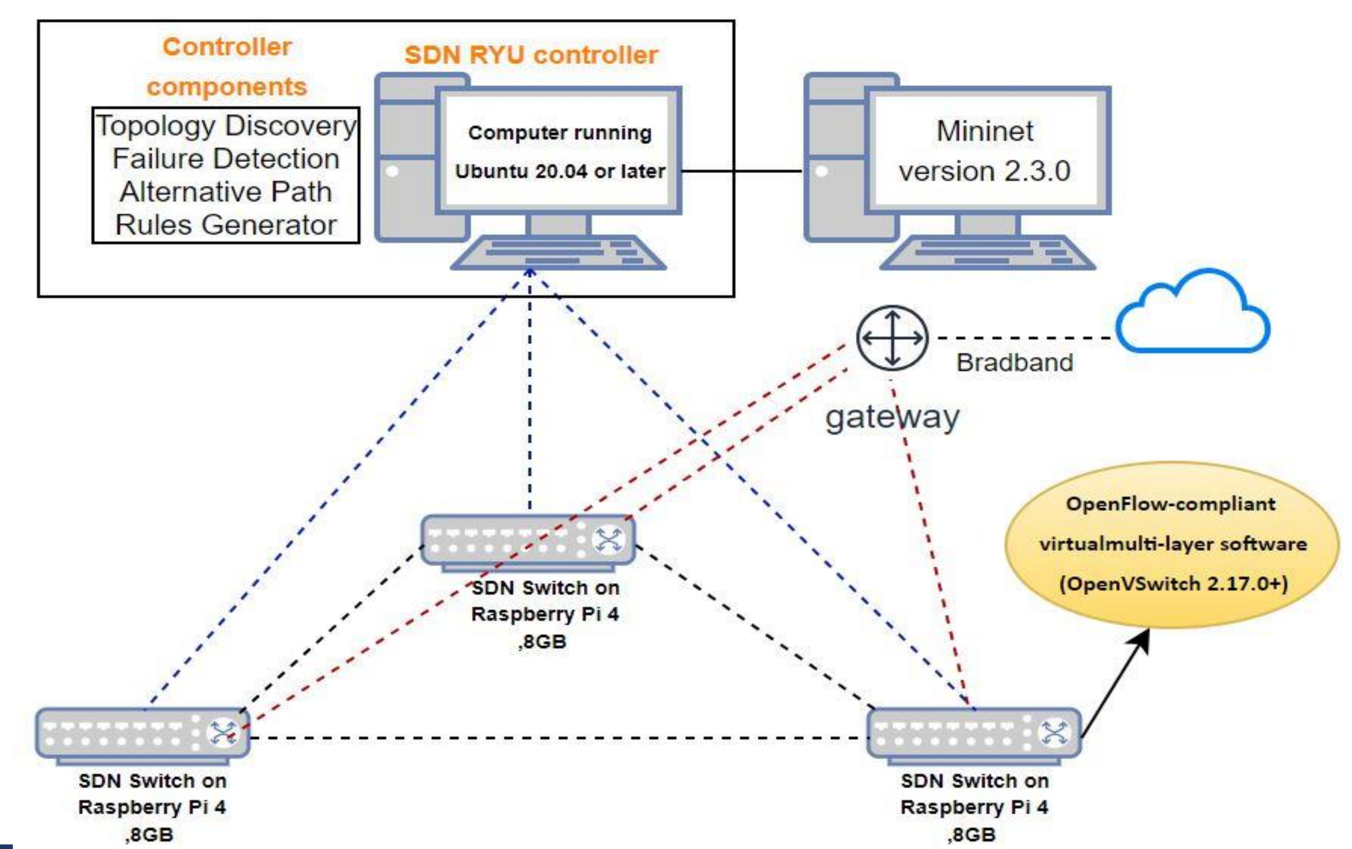
Used to discover and provide topology information about the network, it consistently verifies the topology to address potential link failures. This plays a crucial role in comprehending the network structure and promoting effective communication and management within the network infrastructure.

Network Monitoring Module

Used to enable real-time monitoring of network traffic, including flow statistics, port performance, and available bandwidth, to support network analysis and decision-making processes. It utilizes Open-Flow protocol versions 1.3 for communication with network switches and controllers.

Simulation Setup

Each switch in the network will be linked to a Pycom FiPy board that is compatible with Wi-Fi, LTE-M, NB-IoT, LoRaWAN, and Sigfox.



References

[1] Timon Sloane. Software-defined networking: The new norm for networks – open networking foundation, May 2013.

[2] Christian Berger, Philipp Eichhammer, Hans P. Reiser, Jörg Domaschka, Franz J. Hauck, and Gerhard Habiger. 2021. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. ACM Comput. Surv. 54, 7, Article 147 (September 2022), 39 pages. https://doi.org/10.1145/3462513), sep 2021.